

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES  
(Attorney Docket № 15415US01)**

In the Application of:

Sherman Chen, et al.

Serial № 10/769,173

Filed: January 30, 2004

For: A SECURE KEY AUTHENTICATION  
AND LADDER SYSTEM

Examiner: Yogesh Paliwal

Group Art Unit: 2435

Confirmation № 7811

**Electronically filed on 18-NOV-2009**

**APPEAL BRIEF**

Mail Stop Appeal Brief – Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

This is an appeal from an Office Action dated June 10, 2009 ("Final Office Action"), in which claims 1-41 were finally rejected. The Appellant respectfully requests that the Board of Patent Appeals and Interferences ("Board") reverse the final rejection of claims 1-41 of the present application. The Appellant notes that this Appeal Brief is timely filed within the period for reply that ends on November 19, 2009.

**REAL PARTY IN INTEREST**  
**(37 C.F.R. § 41.37(c)(1)(i))**

Broadcom Corporation, a corporation organized under the laws of the state of California, and having a place of business at 5300 California Avenue, Irvine, California 92617, has acquired the entire right, title and interest in and to the invention, the application, and any and all patents to be obtained therefor, as set forth in the Assignment recorded at Reel 014758, Frame 0483 in the PTO Assignment Search room.

**RELATED APPEALS AND INTERFERENCES**  
**(37 C.F.R. § 41.37(c)(1)(ii))**

The Appellant is unaware of any related appeals or interferences.

**STATUS OF THE CLAIMS**  
**(37 C.F.R. § 41.37(c)(1)(iii))**

The present application includes pending claims 1-41, all of which stand rejected under 35 U.S.C. § 103(a). See the Final Office Action at pages 5-6. The Appellant identifies claims 1-41 as the claims that are being appealed. The text of the pending claims is provided in the Claims Appendix.

**STATUS OF AMENDMENTS**  
**(37 C.F.R. § 41.37(c)(1)(iv))**

The Appellant has not amended any claims subsequent to the final rejection of claims 1-41 mailed on June 10, 2009.

**SUMMARY OF CLAIMED SUBJECT MATTER**  
**(37 C.F.R. § 41.37(c)(1)(v))**

**Independent claim 1 recites the following:**

A method for secure key authentication, the method comprising:

generating at a first location a digital signature of a secure key to obtain a digitally signed secure key<sup>1</sup>;

encrypting the digitally signed secure key utilizing at least a previously generated unreadable digitally signed and encrypted secure key, wherein said previously generated unreadable digitally signed and encrypted secure key was generated by encrypting a previously generated digitally signed secure key<sup>2</sup>; and

transmitting the digitally signed and encrypted secure key from the first location<sup>3</sup>.

**Independent claim 11 recites the following:**

A computer-readable medium having stored thereon, a computer program having at least one code section for secure key authentication, the at least one code section being executable by a machine for causing the machine to perform steps comprising<sup>4</sup>:

generating at a first location a digital signature of a secure key to obtain a digitally signed secure key<sup>5</sup>;

---

<sup>1</sup> See present specification at, e.g., page 11, lines 2-5; (output of 614 in Fig. 6A).

<sup>2</sup> See *id.* at, e.g., page 19, lines 8-22; encryptor 608 (Fig. 6A) uses previously encrypted and signed secure keys (628, 630) generated by encrypting a previously generated digitally signed secure key.

<sup>3</sup> See *id.* at, e.g., page 11, lines 5-6.

<sup>4</sup> See *id.* at, e.g., page 11, lines 18-21.

encrypting the digitally signed secure key utilizing at least a previously generated unreadable digitally signed and encrypted secure key, wherein said previously generated unreadable digitally signed and encrypted secure key was generated by encrypting a previously generated digitally signed secure key<sup>6</sup>; and

transmitting the digitally signed and encrypted secure key from the first location<sup>7</sup>.

**Independent claim 21 recites the following:**

A system for secure key authentication, the system comprising:

at least one processor for generating at a first location a digital signature of a secure key to obtain a digitally signed secure key<sup>8</sup>;

the at least one processor encrypts the digitally signed secure key utilizing at least a previously generated unreadable digitally signed and encrypted secure key, wherein said previously generated unreadable digitally signed and encrypted secure key was generated by encrypting a previously generated digitally signed secure key<sup>9</sup>; and

---

<sup>5</sup> See *id.* at, e.g., page 11, lines 2-5; (output of 614 in Fig. 6A).

<sup>6</sup> See *id.* at, e.g., page 19, lines 8-22; encryptor 608 (Fig. 6A) uses previously encrypted and signed secure keys (628, 630) generated by encrypting a previously generated digitally signed secure key.

<sup>7</sup> See *id.* at, e.g., page 11, lines 18-21.

<sup>8</sup> See *id.* at, e.g., page 11, lines 22-25.

<sup>9</sup> See *id.* at, e.g., page 19, lines 8-22; encryptor 608 (Fig. 6A) uses previously encrypted and signed secure keys (628, 630) generated by encrypting a previously generated digitally signed secure key.

the at least one processor transmitting the digitally signed and encrypted secure key from the first location<sup>10</sup>.

**Independent claim 32 recites the following:**

A system for secure key authentication, the system comprising:

a transmitter<sup>11</sup>;

the transmitter comprises a generator that generates a digital signature of a secure key to obtain a digitally signed secure key<sup>12</sup>;

an encryptor that encrypts the digitally signed secure key utilizing at least a previously generated unreadable digitally signed and encrypted secure key, wherein said previously generated unreadable digitally signed and encrypted secure key was generated by encrypting a previously generated digitally signed secure key<sup>13</sup>; and

the transmitter transmits the digitally signed and encrypted secure key<sup>14</sup>.

**GROUND OF REJECTION TO BE REVIEWED ON APPEAL  
(37 C.F.R. § 41.37(c)(1)(vi))**

Claims 1-41 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over USPP 2002/0001386 ("Akiyama") in view of USP 6,073,237 ("Ellison").

---

<sup>10</sup> See *id.* at, e.g., page 11, lines 25-26.

<sup>11</sup> See *id.* at, e.g., page 12, lines 14-15.

<sup>12</sup> See *id.* at, e.g., page 12, lines 15-17.

<sup>13</sup> See *id.* at, e.g., page 19, lines 8-22; encryptor 608 (Fig. 6A) uses previously encrypted and signed secure keys (628, 630) generated by encrypting a previously generated digitally signed secure key.

<sup>14</sup> See *id.* at, e.g., page 12, line 17.

**ARGUMENT**  
**(37 C.F.R. § 41.37(c)(1)(vii))**

In the Final Office Action, claims 1-41 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over USPP 2002/0001386 ("Akiyama") in view of USP 6,073,237 ("Ellison").

**I. The Proposed Combination of Akiyama and Ellison Does Not Render Claims 1-41 Unpatentable**

**A. Independent Claims 1, 11, 21, and 32**

With regard to the rejection of independent claim 1 under 103(a), the Applicant submits that the combination of Akiyama and Ellison does not disclose or suggest at least the limitation of "encrypting the digitally signed secure key utilizing at least a previously generated unreadable digitally signed and encrypted secure key, wherein said previously generated unreadable digitally signed and encrypted secure key was generated by encrypting a previously generated digitally signed secure key," as recited by the Applicant in independent claim 1. The Final Office Action states the following:

Regarding Claim 1, Akiyama discloses a method for secure key authentication, the method comprising:

generating at a first location (Fig.29, This is a broadcast station where the contents, keys and digital signature for contact information etc, are generated and then sent to receivers) a digital signature (Fig. 5, "Digital signature") of a secure key to obtain a digitally signed secure key (Fig. 5, "work keys", also at paragraph 0107, "The digital signature is information used to check the " authenticity of the contract information, and is used to prevent tampering.", also at paragraph 0107, "The contract information is made up of, e.g., a receiver 10, channel contract information, the

number  $n$  of work keys,  $n$  pairs of work keys and work key identifiers, and digital signature").

encrypting the digitally signed secure key utilizing at least a previously generated unreadable key (Fig. 7, "Enciphered contract information", also at Paragraph 0106, lines 5-8, "The individual control packet is comprised of an information identifier, master key identifier, and encrypted contract information, as shown in FIG. 7.", Note: *[Each digitally signed contract information is encrypted using a master key, also note that master keys are generated and sent to clients via secure card therefore master keys are generated prior to encrypting work keys and it is also unreadable and also secure because only broadcaster and receivers have the master key (see Paragraph 0154)]*)

See the Final Office Action at page 6. The Examiner has used Ellison to teach that a key can be encrypted and signed. Even if we assume that Ellison is combinable with Akiyama (and assume Akiyama's keys can be encrypted and signed), the Applicant points out that Akiyama is still deficient at least for the following reasons.

Referring to FIG. 5 of Akiyama, the Examiner has equated Applicant's "secure key" to Akiyama's "work key", which is part of Akiyama's contract information. Furthermore, Akiyama discloses that a separate master key is used to encrypt the work key, as illustrated in FIG. 3 and further explained in paragraph 0100 of Akiyama. **However, the work keys of Akiyama are different from the master keys, which are used for encrypting the work keys. More specifically, Akiyama's master key is not a previously encrypted and signed work key (i.e., the master key is not generated by encrypting a previously generated signed work key).**

In this regard, Akiyama does not disclose that the work keys (equated by the Examiner to Applicant's "secure key") are encrypted utilizing a previously

**generated unreadable digitally signed and encrypted work key, where the previously generated unreadable digitally signed and encrypted work key was generated by encrypting a previously generated signed work key. In other words, Akiyama does not disclose that the work keys are encrypted using previously generated work keys, as recited in Applicant's claim 1. Ellison does not overcome the above deficiencies of Akiyama.**

Therefore, the Applicant maintains that the combination of Akiyama and Ellison does not disclose or suggest at least the limitation of "encrypting the digitally signed secure key utilizing at least a previously generated unreadable digitally signed and encrypted secure key, wherein said previously generated unreadable digitally signed and encrypted secure key was generated by encrypting a previously generated digitally signed secure key," as recited by the Applicant in independent claim 1.

Accordingly, the proposed combination of Akiyama and Ellison does not render independent claim 1 unpatentable, and a *prima facie* case of obviousness has not been established. The Applicant submits that claim 1 is allowable. Independent claims 11, 21, and 32 are similar in many respects to the method disclosed in independent claim 1. Therefore, the Applicant submits that independent claims 11, 21, and 32 are also allowable over the references cited in the Office Action at least for the reasons stated above with regard to claim 1.



**B. Examiner's Response to Arguments**

**(1). In the 10/28/2008 Non-Final Office Action**

The Examiner states the following in page 3 of the 10/28/2008 Office Action:

Examiner would like to further point out that applicant is trying to force examiner to read the claim such that it would require a secure key and a key that encrypts secure key to be of same type. However, examiner is interpreting the current language of the claim such that as long as the key that encrypt the secure key is also a secure key it reads onto the claimed limitation. Since the master key of Akiyama is only provided to the subscriber through smart cards, the master key of Akiyama is in fact a "secure key". Therefore, the combination of Akiyama and Ellison still discloses all the limitations and the rejection is maintained. Note: examiner would like to further point out that the interpretation taken by applicant that claim require work key to be encrypted using previously generated work keys are not even supported by the specification. Throughout the specification, particularly page 5, lines 22-25 recites, " For example, in the CA system 100 illustrated in FIG. 1, the content scrambling key 118 is protected by the work key 122, which is in turn protected by the master key 126. This key protection "chain" is, sometimes, referred to as a key ladder". Further note that the invention is of a key ladder wherein lower level keys are encrypted using higher level keys. Nowhere in the specification it is recited that same level keys are encrypted using the same level keys as argued by the applicant.

The Applicant submits that claim 1, as presented in the 08/11/08 response, indeed required that a secure key and a key that encrypts the secure key to be of same type. However, to further prosecution and to further clarify this aspect, the Applicant amended independent claims 1, 11, 21 and 32, as set forth in the 03/02/09 response and in the claim listing below. Support for the claim amendments may be found, for example, in Fig. 6A and paragraphs 46-54 of the specification.

More specifically, referring to Applicant's Fig. 6A, the digitally signed secure keys 638 are encrypted by the encryptor 608. The encrypted and signed secure keys 632 are looped back via the registers 610 and then communicated back (628 and 630) to the encryptor 608 for purposes of encrypting the next digitally signed secure key. Obviously, the digitally signed secure keys and the encrypted digitally signed secure keys are of the same type, the difference being that the latter have been encrypted and then looped back for purposes of using them during encryption of subsequent signed secure keys.

In the above citation, the Examiner refers for support to Fig. 1 and page 5, lines 22-25 of the specification. The Examiner further states: "the invention is of a key ladder wherein lower level keys are encrypted using higher level keys. Nowhere in the specification it is recited that same level keys are encrypted using the same level keys as argued by the applicant." The Applicant respectfully disagrees with such characterization of Applicant's invention. The Examiner is encouraged to carefully read the entire specification in light of all Figures. The Applicant is puzzled as to why the Examiner even uses Fig. 1 and page 5 of the specification to judge what Applicant's invention is, since FIGS. 1-4 were clearly marked as PRIOR ART, and pages 1-10 constitute the "Background of the Invention" section. The detailed description of the invention is in pages 15-24 and FIGS. 5-6B of the specification (the Applicant has already briefly summarized Fig. 6A and why the secure key and the key that encrypts the secure key are of the same type).

**(2). In the Current Final Office Action**

The Examiner states the following in pages 2-4 of the Final Office Action:

- Applicant argues that, "More specifically, referring to Applicant's Fig. 6A, the digitally signed secure keys 638 are encrypted by the encryptor 608. The encrypted and signed secure keys 632 are looped back via the registers 610 and then communicated back (628 and 630) to the encryptor 608 for purposes of encrypting the next digitally signed secure key. Obviously, the digitally signed secure keys and the encrypted digitally signed secure keys are of the same type, the difference being that the latter have been encrypted and then looped back for purposes of using them during encryption of subsequent signed secure keys."
- Examiner respectfully disagrees and still maintains that even Fig. 6A does not support applicant interpretation that requires secure key and key that encrypts the secure key to be of same type. See paragraph 0047 (originally filed specification) that recites "In accordance with an aspect of the present invention, the master decryption keys 618 may be utilized in the encryption and decryption of one or more secure keys, for example, a work key and/or a scrambling key." Also note that claim 6 recites, "wherein if the secure key comprises a work key then a decrypted digitally signed master key at the second location is utilized for decrypting an encrypted digitally signed work key.". This claim clearly establishes that when the secure key is a work key it has to be encrypted by the master key. Also see, claim 7 which recites, " wherein if the secure key comprises a scrambling key then a decrypted digitally signed work key at the second location is utilized for decrypting an encrypted digitally signed scrambling key.". Examiner realizes that Fig. 6A in fact shows that after encrypting the secure key do go back to encrypt the next secure keys however, as recited at paragraph 0047 and claims 6 and 7, if the work key is looped back then it will encrypt the content key. Therefore, applicant's interpretation that secure key and key that encrypts the secure key to be of same type is not consistent with the specification and dependent claims 6 and 7. Nowhere in the specification it is recited that same level keys are encrypted using the same level keys as argued by the applicant. Also note that the current claim language does not raise rejection under U.S.C. 112 first paragraph for lacking the written description because at least one interpretation (one taken by the examiner) is supported by the specification. Examiner is interpreting the current language of the claim

such that as long as the key that encrypt the secure key is also a secure key it reads onto the claimed limitation. Further note that even though applicant is interpreting secure key and key that encrypts the secure key to be of same type the current language of the claim is broad enough that as long as the key that encrypt the secure key is also secure it would read onto the claims limitation. Further note that applicant's statement that "Obviously, the digitally signed secure keys and the encrypted digitally signed secure keys are of the same type, the difference being that the latter have been encrypted and then looped back for purposes of using them during encryption of subsequent signed secure keys" appears to be an opinion because there is no written description that requires these keys to be of same type. As clearly shown by paragraph 0047 and claims 6 and 7, key that encrypts the digitally signed key is chosen based on what is the type of the digitally signed key is for example if the digitally signed key is work key then master key is used to encrypt the digitally signed key and if the digitally signed key is a scrambling key then work keys are used to encrypt the digitally signed key (see, paragraph 0041 and claims 6 and 7).

The Applicant respectfully disagrees. The Examiner is primarily relying for support in the above argument to paragraphs 41, 47 (last sentence), and dependent claims 6-7.

The Applicant is confused as to why the Examiner is even mentioning claims 6-7 and paragraph 41 (and related Fig. 5), as this part of Applicant's specification relates to the process of **decryption** the encrypted and digitally signed secure keys, and Applicant's argument pertaining to allowability of claim 1 relates to **how the "previously generated unreadable digitally signed and encrypted secure key" was generated during the process of encryption.**

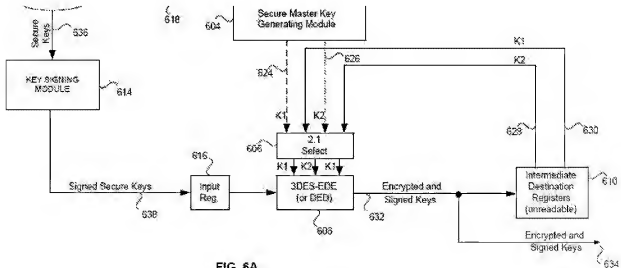
In paragraph 47 (last sentence), the Applicant simply clarifies that the term "secure keys" can include work keys and/or scrambling keys. In a related disclosure, Applicant's claim 4 states that a "secure key" can be a master key, a work key, and/or, a

scrambling key. In other words, **master keys, work keys, and scrambling keys are simply examples of secure keys.**

The Examiner states the following in the above argument:

Nowhere in the specification it is recited that same level keys are encrypted using the same level keys as argued by the applicant.

The Applicant respectfully disagrees with the Examiner's representation above since **this is not what the Applicant argued** (the Applicant did not argue that "same level keys are encrypted using the same level keys"). The Examiner is urged to re-read Applicant's arguments and is now referred to Applicant's Fig. 6A, reproduced in part below:



The relevant portion of Applicant's argument is as follows (annotated with reference to the above Fig. 6A):

Obviously, the digitally signed secure keys (**638 in the above figure 6A**) and the encrypted digitally signed secure keys (**632**) are of the same type, the difference being that the latter have been encrypted and then looped back (**as encrypted and digitally signed secure keys 628, 630**) for purposes of using them during encryption of subsequent signed secure keys.

Again, the issue is not what level keys are used by the encryptor 608 to encrypt a digitally signed secure key 638, as represented by the Examiner. The issue is how the "previously generated unreadable digitally signed and encrypted secure key" (i.e., the digitally signed and encrypted secure key 632 coming as output out of the encryptor 608, being the same as key 628 or 630) is in fact generated. In other words, regardless of whether a master key is used to encrypt a secure "work" key, the result from the encryption is an encrypted "work" key. Similarly, regardless of whether a work key is used to encrypt a secure "scrambling" key, the result from the encryption is an encrypted "scrambling" key. The encryptor 608 simply encrypts a given type of key, but the input and the output of the encryptor 608 remain the same type of key.

The Applicant's argument above is focused on the fact that the encrypted digitally signed and secure key (632, and also 628, 630 – outputs of encryptor 608), regardless of whether it is a work or scrambling key, will obviously be the same type as the digitally signed and secure key (638 – input to encryptor 608). Put another way, the input (638) and the output (any of 632, 628, 630) of the encryptor 608 will have the same type of secure key (e.g., a work key or scrambling key), *regardless* of what type of key is used to encrypt the input key (638).

The Applicant respectfully maintains all arguments stated in the March 2, 2009 response.

**C. Rejection of Dependent Claims 2, 12, 22 and 33**

Claims 2, 12, 22 and 33 depend on independent claims 1, 11, 21 and 32, respectively. Therefore, the Appellant submits that claims 2, 12, 22 and 33 are allowable over the references cited in the Final Office Action at least for the reasons stated above with regard to claims 1, 11, 21 and 32, respectively.

The Appellant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 2, 12, 22 and 33.

**D. Rejection of Dependent Claims 3, 13, 23 and 34**

Claims 3, 13, 23 and 34 depend on independent claims 1, 11, 21 and 32, respectively. Therefore, the Appellant submits that claims 3, 13, 23 and 34 are allowable over the references cited in the Final Office Action at least for the reasons stated above with regard to claims 1, 11, 21 and 32, respectively.

The Appellant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 3, 13, 23 and 34.

**E. Rejection of Dependent Claims 4, 14, 24 and 35**

Claims 4, 14, 24 and 35 depend on independent claims 1, 11, 21 and 32, respectively. Therefore, the Appellant submits that claims 4, 14, 24 and 35 are allowable over the references cited in the Final Office Action at least for the reasons stated above with regard to claim 1, 11, 21 and 32, respectively.

The Appellant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 4, 14, 24 and 35.

**F. Rejection of Dependent Claims 5, 15, 25 and 36**

Claims 5, 15, 25 and 36 depend on independent claims 1, 11, 21 and 32, respectively. Therefore, the Appellant submits that claims 5, 15, 25 and 36 are allowable over the references cited in the Final Office Action at least for the reasons stated above with regard to claim 1, 11, 21 and 32, respectively.

The Appellant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 5, 15, 25 and 36.

**G. Rejection of Dependent Claims 6, 16, 26 and 37**

Claims 6, 16, 26 and 37 depend on independent claims 1, 11, 21 and 32, respectively. Therefore, the Appellant submits that claim 6, 16, 26 and 37 are allowable over the references cited in the Final Office Action at least for the reasons stated above with regard to claims 1, 11, 21 and 32, respectively.

The Appellant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 6, 16, 26 and 37.

**H. Rejection of Dependent Claims 7, 17, 27 and 38**

Claims 7, 17, 27 and 38 depend on independent claims 1, 11, 21 and 32, respectively. Therefore, the Appellant submits that claim 7 is allowable over the references cited in the Final Office Action at least for the reasons stated above with regard to claims 1, 11, 21 and 32, respectively. The Appellant also submits that



Akiyama does not disclose or suggest at least the limitation of "if the secure key comprises a scrambling key, then a decrypted digitally signed work key at the second location is utilized for decrypting an encrypted digitally signed scrambling key," as recited by the Appellant in claims 7, 17, 27 and 38.

With regard to claims 7, 17, 27 and 38, the Final Office Action states the following at page 10:

Regarding Claim 7, the rejection of claim 5 is incorporated and further Akiyama discloses if the secure key comprises a scrambling key then a decrypted digitally signed work key at the second location is utilized for decrypting an encrypted digitally signed scrambling key (Paragraph 0125, lines 9-14, "If the work key can be acquired, information of an encrypted section in the common control packet is decrypted using the work key (step 844). A channel key Kch is acquired from the decrypted information, and is stored in the channel key storage 118")

The Examiner, in the above arguments, has already equated Appellant's "secure key" to Akiyama's work key in Fig. 5. However, the above cited portion of Akiyama (paragraph 0125) does not disclose that the contract information of Fig. 5 includes a scrambling key. Akiyama only discloses that the contract information of Fig. 5 includes a work key, not a scrambling key. In addition, Akiyama's step S44 does not disclose that a decrypted digitally signed work key is used for purposes of decrypting an encrypted and digitally signed scrambling key. Accordingly, the Appellant submits that claims 7, 17, 27 and 38 are allowable over the references cited in the Final Office Action at least for the above reasons.

The Appellant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 7, 17, 27 and 38.

**I. Rejection of Dependent Claims 8, 18, 28 and 39**

Claims 8, 18, 28 and 39 depend on independent claims 1, 11, 21 and 32, respectively. Therefore, the Appellant submits that claims 8, 18, 28 and 39 are allowable over the references cited in the Final Office Action at least for the reasons stated above with regard to claims 1, 11, 21 and 32, respectively.

The Appellant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 8, 18, 28 and 39.

**J. Rejection of Dependent Claims 9, 19, 29 and 40**

Claims 9, 19, 29 and 40 depend on independent claims 1, 11, 21 and 32, respectively. Therefore, the Appellant submits that claims 9, 19, 29 and 40 are allowable over the references cited in the Final Office Action at least for the reasons stated above with regard to claims 1, 11, 21 and 32, respectively.

The Appellant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 9, 19, 29 and 40.

**K. Rejection of Dependent Claims 10, 20, 30 and 41**

Claims 10, 20, 30 and 41 depend on independent claims 1, 11, 21 and 32, respectively. Therefore, the Appellant submits that claims 10, 20, 30 and 41 are allowable over the references cited in the Final Office Action at least for the reasons stated above with regard to claims 1, 11, 21 and 32, respectively.

The Appellant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 10, 20, 30 and 41.

**L. Rejection of Dependent Claim 31**

Claim 31 depends on independent claim 21. Therefore, the Appellant submits that claim 31 is allowable over the references cited in the Final Office Action at least for the reasons stated above with regard to claim 21.

The Appellant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claim 31.

### CONCLUSION

For at least the foregoing reasons, the Appellant submits that claims 1-41 are in condition for allowance. Reversal of the Examiner's rejection and issuance of a patent on the application are therefore requested.

The Commissioner is hereby authorized to charge \$540 (to cover the Brief on Appeal Fee) and any additional fees or credit any overpayment to the deposit account of McAndrews, Held & Malloy, Ltd., Account No. 13-0017.

Respectfully submitted,

Date: 18-NOV-2009

By: /Ognyan I. Beremski/  
Ognyan Beremski, Reg. No. 51,458  
Attorney for Appellant

McANDREWS, HELD & MALLOY, LTD.  
500 West Madison Street, 34th Floor  
Chicago, Illinois 60661  
Telephone: (312) 775-8000  
Facsimile: (312) 775 – 8100

(OIB)

**CLAIMS APPENDIX**  
**(37 C.F.R. § 41.37(c)(1)(viii))**

1. A method for secure key authentication, the method comprising:  
generating at a first location a digital signature of a secure key to obtain a digitally signed secure key;  
encrypting the digitally signed secure key utilizing at least a previously generated unreadable digitally signed and encrypted secure key, wherein said previously generated unreadable digitally signed and encrypted secure key was generated by encrypting a previously generated digitally signed secure key; and  
transmitting the digitally signed and encrypted secure key from the first location.
2. The method according to claim 1, comprising generating the digital signature from at least one of an asymmetric encryption algorithm and a symmetric encryption algorithm.
3. The method according to claim 1, comprising encrypting the digitally signed secure key prior to transmission utilizing at least an encrypted master key, to obtain the digitally signed and encrypted secure key.
4. The method according to claim 3, wherein the secure key comprises at least one of a master key, a work key and a scrambling key.

5. The method according to claim 1, comprising:  
receiving the digitally signed and encrypted secure key at a second location; and  
decrypting the digitally signed and encrypted secure key to obtain a decrypted  
digitally signed secure key.

6. The method according to claim 5, wherein if the secure key comprises a  
work key, then a decrypted digitally signed master key at the second location is utilized  
for decrypting an encrypted digitally signed work key.

7. The method according to claim 5, wherein if the secure key comprises a  
scrambling key, then a decrypted digitally signed work key at the second location is  
utilized for decrypting an encrypted digitally signed scrambling key.

8. The method according to claim 5, comprising verifying authenticity of the  
digital signature of the digitally signed and encrypted secure key.

9. The method according to claim 8, comprising verifying the authenticity of  
the digital signature utilizing at least one of an asymmetric decryption algorithm and a  
symmetric decryption algorithm.

10. The method according to claim 8, comprising determining whether to  
verify authenticity of the digital signature.

11. A computer-readable medium having stored thereon, a computer program having at least one code section for secure key authentication, the at least one code section being executable by a machine for causing the machine to perform steps comprising:

generating at a first location a digital signature of a secure key to obtain a digitally signed secure key;

encrypting the digitally signed secure key utilizing at least a previously generated unreadable digitally signed and encrypted secure key, wherein said previously generated unreadable digitally signed and encrypted secure key was generated by encrypting a previously generated digitally signed secure key; and

transmitting the digitally signed and encrypted secure key from the first location.

12. The computer-readable medium according to claim 11, comprising code for generating the digital signature from at least one of an asymmetric encryption algorithm and a symmetric encryption algorithm.

13. The computer-readable medium according to claim 11, comprising code for encrypting the digitally signed secure key prior to transmission utilizing at least an encrypted master key, to obtain the digitally signed and encrypted secure key.

14. The computer-readable medium according to claim 13, wherein the secure key comprises at least one of a master key, a work key and a scrambling key.

15. The computer-readable medium according to claim 11, comprising:  
code for receiving the digitally signed and encrypted secure key at a second location; and

code for decrypting the digitally signed and encrypted secure key to obtain a decrypted digitally signed secure key.

16. The computer-readable medium according to claim 15, wherein if the secure key comprises a work key, then a decrypted digitally signed master key at the second location is utilized for decrypting an encrypted digitally signed work key.

17. The computer-readable medium according to claim 15, wherein if the secure key comprises a scrambling key, then a decrypted digitally signed work key at the second location is utilized for decrypting an encrypted digitally signed scrambling key.

18. The computer-readable medium according to claim 15, comprising code for verifying authenticity of the digital signature of the digitally signed and encrypted secure key.



19. The computer-readable medium according to claim 18, comprising code for verifying the authenticity of the digital signature utilizing at least one of an asymmetric decryption algorithm and a symmetric decryption algorithm.

20. The computer-readable medium according to claim 18, comprising code for determining whether to verify authenticity of the digital signature.

21. A system for secure key authentication, the system comprising:  
at least one processor for generating at a first location a digital signature of a secure key to obtain a digitally signed secure key;

the at least one processor encrypts the digitally signed secure key utilizing at least a previously generated unreadable digitally signed and encrypted secure key, wherein said previously generated unreadable digitally signed and encrypted secure key was generated by encrypting a previously generated digitally signed secure key;  
and

the at least one processor transmitting the digitally signed and encrypted secure key from the first location.

22. The system according to claim 21, the at least one processor generating the digital signature from at least one of an asymmetric encryption algorithm and a symmetric encryption algorithm.

23. The system according to claim 21, the at least one processor encrypting the digitally signed secure key prior to transmission utilizing at least an encrypted master key, to obtain the digitally signed and encrypted secure key.

24. The system according to claim 23, wherein the secure key comprises at least one of a master key, a work key and a scrambling key.

25. The system according to claim 21, the at least one processor:  
receiving the digitally signed and encrypted secure key at a second location; and  
decrypting the digitally signed and encrypted secure key to obtain a decrypted digitally signed secure key.

26. The system according to claim 25, wherein a decrypted digitally signed master key at the second location is utilized for decrypting an encrypted digitally signed work key.

27. The system according to claim 25, wherein a decrypted digitally signed work key at the second location is utilized for decrypting an encrypted digitally signed scrambling key.

28. The system according to claim 25, the at least one processor verifying authenticity of the digital signature of the digitally signed and encrypted secure key.

29. The system according to claim 28, the at least one processor verifying the authenticity of the digital signature utilizing at least one of an asymmetric decryption algorithm and a symmetric decryption algorithm.

30. The system according to claim 28, the at least one processor determining whether to verify authenticity of the digital signature.

31. The system according to claim 21, wherein the at least one processor comprises at least one of a host processor, a microprocessor, and a microcontroller.

32. A system for secure key authentication, the system comprising:  
a transmitter;  
the transmitter comprises a generator that generates a digital signature of a secure key to obtain a digitally signed secure key;  
an encryptor that encrypts the digitally signed secure key utilizing at least a previously generated unreadable digitally signed and encrypted secure key, wherein said previously generated unreadable digitally signed and encrypted secure key was generated by encrypting a previously generated digitally signed secure key; and  
the transmitter transmits the digitally signed and encrypted secure key.

33. The system according to claim 32, wherein the generator generates the digital signature from at least one of an asymmetric encryption algorithm and a symmetric encryption algorithm.

34. The system according to claim 32, wherein the encryptor encrypts the digitally signed secure key prior to transmission utilizing at least an encrypted master key, to obtain the digitally signed and encrypted secure key.

35. The system according to claim 34, wherein the secure key comprises at least one of a master key, a work key and a scrambling key.

36. The system according to claim 32, comprising:  
a receiver that receives the digitally signed secure key; and  
the receiver comprising a decryptor that decrypts the digitally signed secure key to obtain a decrypted digitally signed secure key.

37. The system according to claim 36, wherein the receiver comprises a decryptor that utilizes a digitally signed master key to decrypt an encrypted digitally signed work key.

38. The system according to claim 36, wherein the decryptor utilizes a decrypted digitally signed work key to decrypt an encrypted digitally signed scrambling key.

39. The system according to claim 36, the receiver comprises a verifier that verifies authenticity of the digital signature of the digitally signed and encrypted secure key.

40. The system according to claim 39, wherein the verifier utilizes at least one of an asymmetric decryption algorithm and a symmetric decryption algorithm.

41. The system according to claim 39, wherein the verifier determines whether to verify authenticity of the digital signature.

**EVIDENCE APPENDIX**  
**(37 C.F.R. § 41.37(c)(1)(ix))**

- (1) United States Patent App. Pub. 2002/0001386 ("Akiyama"), entered into record by the Examiner in the March 13, 2007 Office Action.
- (2) United States Patent No. 6,073,237 ("Ellison"), entered into record by the Examiner in the November 14, 2007 Office Action.

**RELATED PROCEEDINGS APPENDIX**  
**(37 C.F.R. § 41.37(c)(1)(x))**

The Appellant is unaware of any related appeals or interferences.